ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 4, April 2012

An Efficient Secure AODV Routing Protocol in MANET

Durgesh Wadbude, Vineet Richariya

***Abstract:** An ad-hoc network is a multi-hop wireless network where all nodes cooperatively maintain network connectivity without a centralized infrastructure. If these nodes change their positions dynamically, it is called a mobile ad-hoc network (MANET). Since the network topology changes frequently, efficient adaptive routing protocols such as AODV, DSR are used. As the network is wireless, security becomes the major issue in Mobile Ad hoc Networks. Some of the attacks such as modification, fabrication, impersonation and denial of service attacks are due to misbehavior of malicious nodes, which disrupts the transmission. In this paper we proposed an efficient secure AODV routing protocol. Simulation results show that our proposed routing algorithm provides a better level of security and performance than existing works. The simulation results show the improvement of the network performance, in terms of overhead, and end to end delay to the secure AODV routing protocol.*

Keywords- **MANET, AODV, Secure AODV, Routing Protocol.**

I. INTRODUCTION

MANET is a highly challenged network environment due to its special characteristics such as decentralization, dynamic topology and neighbor based routing. MANET can be applied to situations where an infrastructure is unavailable or deploying one is not cost effective. Such situations include disaster recovery, military field's communications, or some other crisis management services. The topology of MANET may change uncertainly and rapidly due to high mobility of the independent mobile nodes. Because of network decentralization, each node in MANET would act as a "router" to discover a routing path or to forward the data packets. Unlike wired networks, the functional design of MANET must take into account many factors such as wireless link quality, power limitation, and multi-user interference and so on [1] and [2].

There are numerous kinds of attacks in the mobile ad hoc network, almost all of which can be classified as the following types: External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors [3]. The security mechanism for MANET, on one hand, must require low computation complexity and a small number of appended messages to save the node energy. On the other hand, it should also be competitive and effective in preventing misbehaviors or identifying misbehaving nodes from normal ones. In this paper we proposed an efficient secure AODV routing protocol. The objective of proposed SAODV routing protocol is to secure routing packets of AODV protocol in MANET. The AODV protocol's routing have been improved to secure AODV.

II. BACKGROUND TECHNIQUES

AODV:

The Ad hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multihop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. AODV allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication. AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner. The operation of AODV is loop-free, and by avoiding the Bellman-Ford "counting to infinity" problem offers quick convergence when the ad-hoc network topology changes (typically, when a node moves in the network). When links break, AODV causes the affected set of nodes to be notified so that they are able to invalidate the routes using the lost link. One distinguishing feature of AODV is its use of a destination sequence number for each route entry. The destination sequence number is created by the destination to be included along with any route information it sends to requesting nodes. Using destination sequence numbers ensures loop freedom and is simple to program. Given the choice between two routes to a destination, a requesting node is required to select the one with the greatest sequence number [1] and [2].

A. Working of AODV:

Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV. These message types are received via UDP, and normal IP header processing applies. So, for instance, the requesting node is expected to use its IP address as the Originator IP address for the messages. For broadcast messages, the IP limited broadcast address (255.255.255.255) is used. This means that such messages are not blindly forwarded. However, AODV operation does require certain messages (e.g., RREQ) to be disseminated widely, perhaps throughout the ad hoc network. The range of dissemination of such RREQs is indicated by the TTL in the IP header. Fragmentation is typically not required. As long as the endpoints of a communication connection have valid routes to each other, AODV does not play any role. When a route to a new destination is needed, the node broadcasts a RREQ to find a route to the destination. A route can be determined when the RREQ reaches either the destination itself, or an intermediate node with a 'fresh enough' route to the destination. A 'fresh enough' route is a valid route entry for the destination whose associated sequence number is at least as great as that contained in the RREQ. The route is made available by unicasting a RREP back to the origination of the RREQ. Each node receiving the request caches a route back to the originator of the request, so that the RREP can be unicast from the destination along a path to that originator, or likewise from any intermediate node that is able to satisfy the request. Nodes monitor the link status of next hops in active routes. When a link break in an active route is detected, a RERR message is used to notify other nodes that the loss of that link has occurred. The RERR message indicates those destinations (possibly subnets) which are no longer reachable by way of the broken link. In order to enable this reporting mechanism, each node keeps a "precursor list", containing the IP address for each its neighbors that are likely to use it as a next hop towards each destination. The information in the precursor lists is most easily acquired during the processing for generation of a RREP message, which by definition has to be sent to a node in a precursor list. If the RREP has a nonzero prefix length, then the originator of the RREQ which solicited the RREP information is included among the precursors for the subnet route (not specifically for the particular destination).

A RREQ may also be received for a multicast IP address. In this document, full processing for such messages is not specified. For example, the originator of such a RREQ for a multicast IP address may have to follow special rules. However, it is important to enable correct multicast operation by intermediate nodes that are not enabled as originating or destination nodes for IP multicast address, and likewise are not equipped for any special multicast protocol processing. For such multicast-unaware nodes, processing for a multicast IP address as a destination IP address MUST be carried out in the same way as for any other destination IP address [4] and [5]. AODV is a routing protocol, and it deals with route table management. Route table information must be kept even for short-lived routes, such as are created to temporarily store reverse paths towards nodes originating RREQs. AODV uses the following fields with each route table entry:

→Destination IP Address

→Destination Sequence Number

→Valid Destination Sequence Number flag

→Other state and routing flags (e.g., valid, invalid, repairable, being repaired)

→ Network Interface

→ Hop Count (number of hops needed to reach destination)

→ Next Hop

→List of Precursors

→ Lifetime (expiration or deletion time of the route)

Managing the sequence number is crucial to avoiding routing loops, even when links break and a node is no longer reachable to supply its own information about its sequence number. A destination becomes unreachable when a link breaks or is deactivated. When these conditions occur, the route is invalidated by operations involving the sequence number and marking the route table entry state as invalid [3] and [8].

III. RELATED WORK

A. Security Aware Ad hoc Routing (SAR)

SAR protocol integrates the trust level of a node and the security attributes of a route to provide the integrated security metric for the requested route. A Quality of Protection (QoP) vector used is a combination of security level and available cryptographic techniques. It uses the timestamps and sequence numbers to stop the replay attacks. Interception and subversion threats can be prevented by trust level key authentication. Attacks like modification and fabrication can be stopped by verifying the digital signatures of the transmitted packet. The main drawbacks of using SAR are that it required excessive encrypting and decrypting at each hop during the path discovery. The discovered route may not be the shortest route in the terms of hop-count, but it is secure [2] and [7].

B. Trusted Ad-hoc On-demand distance vector Routing (TAODV)

TAODV is secure routing protocol which uses cryptography technologies recommended to take effect before nodes in the establish trust relationships among one another. The main salient feature of TAODV is that using trust relationships among nodes, there is no need for a node to request and verify certificates all the time. TAODV (Trusted AODV) has several salient features:

(1) Nodes perform trusted routing behaviors mainly according to the trust relationships among them;

(2) A node that performs malicious behaviors will eventually be detected and denied to the whole network.

(3) The performance of the System is improved by avoiding requesting and verifying certificates at every routing step.

That protocol greatly reduces the computation overheads. Assume that the keys and certificates needed by these cryptographic technologies have been obtained through some key management procedures before the node performs routing behaviors. Some extra new fields are added into a node's routing table to store its opinion about other nodes' trustworthiness and to record the positive and negative evidences when it performs routing with others. The main advantages of embedding trust model into the routing layer of MANET, save the consuming time without the trouble of maintaining expire time, valid state, etc. which is important in the situation of high node mobility and invalidity. Trusted AODV are mainly three modules in the whole TAODV system: basic AODV routing protocol, trust model, and trusted AODV routing protocol. Based on trust model, the TAODV routing protocol contains such procedures as trust recommendation, trust combination, trust judging, cryptographic routing behaviors, trusted routing behaviors, and trust updating [1] and [6] and [9].

C. ARAN (Authenticated Routing for Ad-hoc Networks)

ARAN provides authentication, message integrity and non-repudiation in ad-hoc networks by using a preliminary certification process which is followed by a route instantiation process that ensures end-to-end security services. But it needs the use of trusted certification server. The main disadvantage with the protocol is every node that forwards a route discovery or a route reply message must also sign it, which is very power consuming and causes the size of the routing messages to increase at each hop.

It is clear from the above mentioned security analysis of the ARAN protocol that ARAN is a secure MANET routing protocol providing authentication, message integrity, confidentiality and non-repudiation by using certificates infrastructure. As a consequence, ARAN is capable of defending itself against spoofing, fabrication, modification, DoS and disclosure attacks. However, erratic behavior can come from a malicious node, which will be defended against successfully by existing ARAN protocol, and can also come from an authenticated node. The currently existing ARAN secure routing protocol does not account for attacks that are conducted by authenticated selfish nodes as these nodes trust each other to cooperate in providing network functionalities. This results in that ARAN fails to detect and defend against an authenticated selfish node participating in the mobile ad hoc network. Thus, if an authenticated selfish node does not forward or intentionally drop control or data packets, the current specification of ARAN routing protocol cannot detect or defend against such authenticated selfish nodes. This weakness in ARAN specification will result in the disturbance of the ad hoc network and the waste of the network bandwidth [8] and [10].

IV. PROPOSED SECURE ROUTING PROTOCOL

The objective of proposed SAODV routing protocol is to secure routing packets of AODV protocol in MANET. The AODV protocol’s routing have been improved to secure AODV. The proposed SAODV have three components. These are Hash Chain, Digital Signature, and Protocol Enforcement Mechanism.

1. Hash Chain used for securing the hop count
2. Digital Signature for authentication
3. Protocol Enforcement Mechanism using the enforcement this protocol will address of any nodes, which packets have been changes.

A.SAODV Hash Chains

Hash chains are used in SAODV to authenticate the hop count of the AODV routing messages (not only by the end points, but by any node that receives one of those messages. Every time a node wants to send a RREQ or a RREP it generates a random number (seed). Select a Maximum Hop Count. Maximum Hop Count SHOULD be set to the TTL value in the IP header, and SHOULD never exceed its configuration parameter NET_DIAMETER.The Hash field in the Signature Extension is set to the seed. The Top Hash field is set to the seed hashed Max Hop Count times. Every time a node receives a RREQ or a RREP it verifies the hop count by hashing Max Hop Count Hop Count times the Hash field, and checking that the resultant value is the same than the Top Hash. If the check fails, the node SHOULD drop the packet. Before rebroadcast a RREQ or forwarding a RREP, a node hashes one time the Hash field in the Signature Extension.

The function used to compute the hash is set in the Hash Function field. Since this field is signed, a forwarding node will only be able to use the same hash function that the originator of the routing message has selected. If a node cannot verify or forward a routing message because it does not support the hash function that has been used, then it drops the packet.

B.SAODV Signatures

When calculating signatures, Hop Count field is always zeroed, because it is a mutable field. In the case of the Signature for RREP field of the RREQ Double Signature Extension, what is signed is the future RREP message that nodes might send back in response to the RREQ. To construct this message it uses the values of the RREQ and the Prefix Size (the RREP field that is not derivable from the RREQ but not zeroed when computing the signature. In the case of RREPs, R and A flags are also zeroed. SAODV is not designed taking into account AODV multicast ('R' flag is used in multicast) and 'A' flag is mutable and, if an attacker alters it, it can only lead to some sort of denial of service. Every time a node generates a RREQ it decides if it should be signed with a Single Signature Extension or with a Double Signature Extension. All implementations MUST support RREQ Single Signature Extension, and SHOULD support RREQ Double Signature Extension. A node that generates a RREQ with the gratuitous RREP flag set SHOULD sign the RREQ with a Double Signature Extension. A node SHOULD never generate a RREQ without adding a Signature Extension. When a node receives a RREQ, first verify the signature before creating or updating a reverse route to that host. Only if the signature is verified, it will store the route. If the RREQ was received with a Double Signature Extension, then the node will also store the signature, the lifetime and the Destination IP address for the RREP in the route entry. If a node receives a RREQ without a Signature Extension it SHOULD drop it. An intermediate node will reply a RREQ with a RREP only if fulfills the AODV requirements to do so, and the node has the corresponding signature and the old lifetime and old originator IP address to put into the 'Signature', 'Old Lifetime' and 'Old Originator IP address' fields of the RREP Double Signature Extension. Otherwise, it will rebroadcast the RREQ. When a RREQ is received by the destination itself, it will reply with a RREP only if fulfills the AODV requirements to do so. This RREP will be sent with a RREP Single Signature Extension. All implementations MUST support RREP Single Signature Extension, and SHOULD support RREP Double Signature Extension. A node SHOULD never generate a RREP without adding a Signature Extension. This also applies to gratuitous RREPs. When a node receives a RREP, first verifies the signature before creating or updating a route to that host. Only if the signature is verified, it will store the route with the signature and the lifetime and the originator IP address of the RREP. If a node receives a RREP without a Signature Extension it SHOULD drop it. Every node, generating or forwarding a RERR message, uses digital signatures to sign the whole message and any neighbor that receives verifies the signature.

C.The assumption of proposed SAODV routing protocol are:

1. The destination node can authenticate packets from the originator and each of receiving nodes can authenticate packets from the previous packets.
2. The hop count value is protecting using hash chain. It cannot be reduced by malicious node, but could be increased by one or retained unchanged.
3. Nodes in the network have capabilities for keys like private key, public key creation, signature generation and its verification.
4. Each node has one pair of keys (private key& public key). The digital signature algorithm is well by the entire node in the network.

D. The Proposed SAODV Algorithms to handle the routing packets:

Algorithm1: Receiving RREQ Packets from the originator

```
//
1.  Start
2.  Packet Classifier ← Packets
3.  If (RREQ secure)
4.  Packet extractor ← RREQ secure
5.  Packets: Original RREQ + Hash Chin protection created in node + digital signature + protection Key.
6.  Hop count tester ← hop count + max hop + top hash
7.  Signature verification ← Protection key + digital signature
8.  If (hop count tester and signature verification is matched)
9.  Then update route
10. End if
11. If (node = destination)
12. Signature generate ← non mutable RREQ
13. Hash chain generate ←0; packet Builder → RREP + Hash Chain protection + digital signature + protection key
14. Sent RREP to lower layer
15. Else
16. Packet forward ← RREQ
17. End if
//
```

Algorithm 2: Broadcast RREQ packet

```
//
1.  Start
2.  Packet destination ← RREQ
3.  Next hop = find the as packet destination
4.  If (next hop= null)
5.  Then
6.  Packet forword ← RREQ
7.  Else
8.  Signature generator ← non  table RREQ
9.  Hash chain protect generator ← 0;
10. Packet bulder ← RREQ + hash chain protection + digital signature + protection key of the node
11. Broadcast
12. End if
//
```

Algorithm 3: Receiving RREP packets

```
1.  Start
2.  Packet destination = extractor ← RREP
3.  Packet origin= extractor ← RREP
4.  *//Route entry for find this node (destination) //*
5.  If (route entry = null)
6.  Addition route as routing success
7.  Else
8.  Routing not success
9.  End if
10. If(node address= packet destination)
11. Generate RREP and receiving RREQ algorithm
12. Else
13. Forward packet in next node in the route
14. Forwarding route reply
15. End if
16. End if
//
```

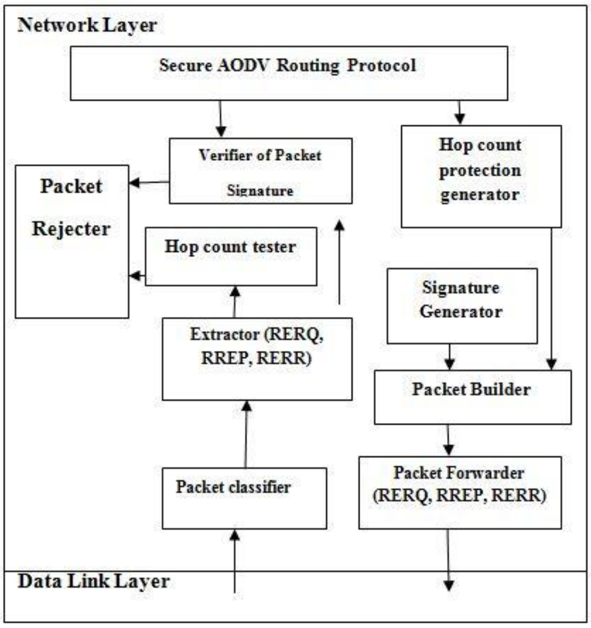
Network Layer
Secure AODV Routing Protocol
Verifier of Packet Signature
Hop count protection generator
Packet Rejecter
Hop count tester
Signature Generator
Extractor (RERQ, RREP, RERR)
Packet Builder
Packet classifier
Packet Forwarder (RERQ, RREP, RERR)
Data Link Layer

Fig 1: Architecture of Secure AODV routing protocol

Packet arrive to the system will be identified by the packet classifier to determine the type of packet. This protocol has four packet types. These are Route Request Secure (RREQ), Route Reply Secure (RREP), Route Error Secure (RERR) and Hello Packet. All packets except the hello packets will be extracted to identify component within the packets. This will be followed by the integrity evaluation and hop count verification of the extracted packets. Two modules; these are the packet signature verification and hop count tester will handle these task. Also at this point, the RERR Secure is executed from the hop count verification as this packet has no hop count, but integrity evaluation is still considered on this packet. Any alternation to the hop counts of RREQ Secure and RREP secure either by incrementing or decrementing the value will trigger the hop count tester to generate error notification and will reject the packet through packet rejecter. The violation of the packet integrity will also trigger error notification and will reject the packet reject too. If the evaluation and verification are succeeding, this protocol may update routing information to routing table. Before passing the packet, call hop count protection generator hash from, and then the packet builder warps the signature, hop count protection, and public key into secure packet and pass them to packet forwarder.

V. RESULTS ANALYSIS

A. Simulation Parameters:

We proposed Secure Routing Protocol algorithm in AODV was successfully implemented using NS2 simulator, in which I have implemented the algorithm in existing techniques by making necessary changes in the existing system. The simulation parameters of our thesis work as follows:

Table 1: Simulation parameters

Length of Wireless Network	500 (M)
No. of mobile nodes	10-60
Packet rate of normal connection	1
Movement Model	Random Waypoint
Traffic type	CBR, HTTP, FTP
Max. mode speed	5 m/s – 20 m/s
No. of connections between nodes	5 – 20
Pause time	10 s
Rate (packet per sec)	2 packets/s
Data payload (packet size)	28 – 512 bytes

The random waypoint model is chosen for movement patterns. In the random waypoint model of mobility, nodes choose a destination and move in a straight line toward the destination at a speed uniformly distributed between 0 meters/second (m/s) and some maximum speed. When a node reaches its destination, it stays during a specified period of time called pause time, chooses a new destination and begins moving towards it immediately in the same speed.

B, Performance Metrics:

The performance metrics used for the comparison are the same as those used for evaluating the SAODV (Secure Routing Protocol in AODV) and ARAN (Authenticated Routing for Ad-hoc Networks). We measured the key parameters to evaluate the performance of metrics as follows:

➔ ***Route discovery packets (overhead)*** are defined as the number of all packets generated by all nodes in the network in order to establish routes between sources and destinations. The figure2 describe the route discovery packets vs. number of nodes. The red line indicates proposed routing protocol SAODV performance which is more efficient than ARAN (blue line) performance.

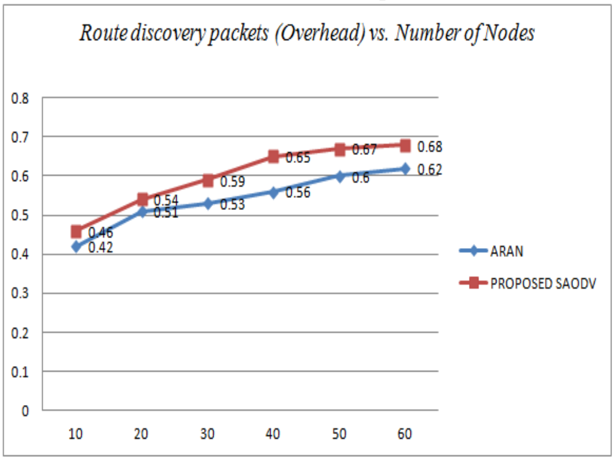

Fig 2: Route discovery packets (Overhead) vs. Number of Nodes

➔***Average end-to-end delay*** of transferred data packets includes all possible delays caused by buffering during route discovery, queuing at the interface-queue and retransmission delays at the medium access control layer.

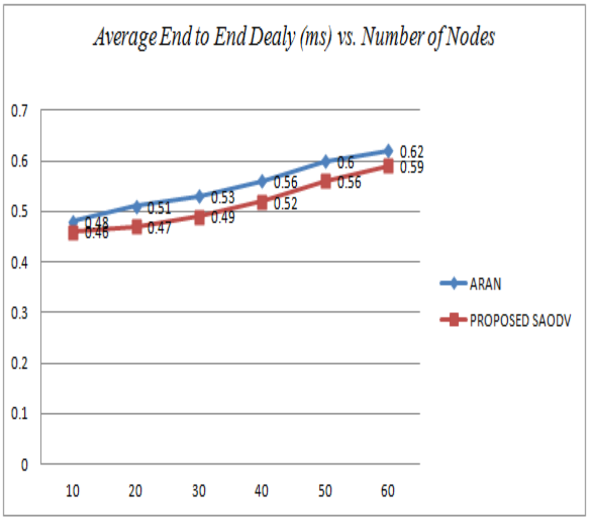

Fig 3: Average End to End Delay (ms) vs. Number of Nodes

The figure3 describe the Average End to End Delay (ms) vs. Number of Nodes. The red line indicates proposed routing protocol SAODV performance which is more efficient than ARAN (blue line) performance with respect to end to end delay. In terms of the scalability of the network by increasing the number of nodes, Secure Routing protocol in AODV performs better than ARAN; because it selects the only nodes have the secure path with strongest link as the next hop towards the destination.

VI. CONCLUSION

In this paper the proposed approach uses improved of security mechanisms to introduce in the proposed techniques so that it satisfies the main security requirement and guarantees the discovery of a correct and secure route. The security mechanisms that the protocol uses are the hash chain, digital signature and Protocol Enforcement Mechanism. The performance of these two protocols (SAODV and ARAN) was tested in simulation and their communication costs were measured using the NS-2 simulator, which was suitable for the present purpose. The evaluation metrics used in this study were overhead and end to end delay, both the cases our protocol show better performance.

REFERENCES

[1] R. S. Mangrulkar, Pallavi V Chavan and S. N. Dagadkar, “Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for MaNeT”, International Journal of Computer Applications (0975 – 8887) Volume 7– No.10, October 2010, pp 36-39.

[2] Shilpa S G, Mrs. N.R. Sunitha, B.B. Amberker, “A Trust Model for Secure and QoS Routing in MANETS”, INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY & CREATIVE ENGINEERING (ISSN:2045-8711) VOL.1 NO.5MAY 2011, pp 22-31.

[3] Suchita Gupta, Ashish Chourey, “ PERFORMANCE EVALUATION OF AODV PROTOCOL UNDER PACKET DROP ATTACKS IN MANET”, International Journal of Research in Computer Science eISSN 2249-8265 Volume 2 Issue 1 (2011) pp. 21-27.

[4] A.Menaka Pushpa M.E., “Trust Based Secure Routing in AODV Routing Protocol”, IEEE2009.

[5] Songbai Lu1, Longxuan Li and Kwok-Yan Lam, Lingyan Jia, “SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack”, IEEE 2009 International Conference on Computational Intelligence and Security, pp 421-425.

[6] Ming Yu, Mengchu Zhou, and Wei Su, “A Secure Routing Protocol against Byzantine Attacks for MANETs in Adversarial Environments”, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 1, JANUARY 2009.

[7] Victor, C., Francisco, J., Pedro, M. 2009, Simulation-based Study of Common Issues in VANET Routing Protocols. IEEE 69th Vehicular Technology Conference, VTC2000.

[8] Wenjing, W., X. Fei, et al. 2007, TOPO: Routing in Large Scale Vehicular Networks, IEEE 66th Vehicular Technology Conference, and VTC-2007.

[9] Wenjing, W., X. Fei, et al. 2007, An Integrated Study on Mobility Models and Scalable Routing Protocols in VANETs. 2007 Mobile Networking for Vehicular Environments.

[10] Abedi, O., M. Fathy, et al. 2008, Enhancing AODV routing protocol using mobility parameters in VANET, IEEE/ACS International Conference on Computer Systems and Applications, AICCSA 2008.